



GSX
GLOBAL
SECURITY
EXPERTS

標的型攻撃マルウェア(BOT)発見サービス

グローバルセキュリティエキスパート株式会社

標的型攻撃の特徴

近年、機密情報の取得などを目的とした「標的型攻撃」が多発

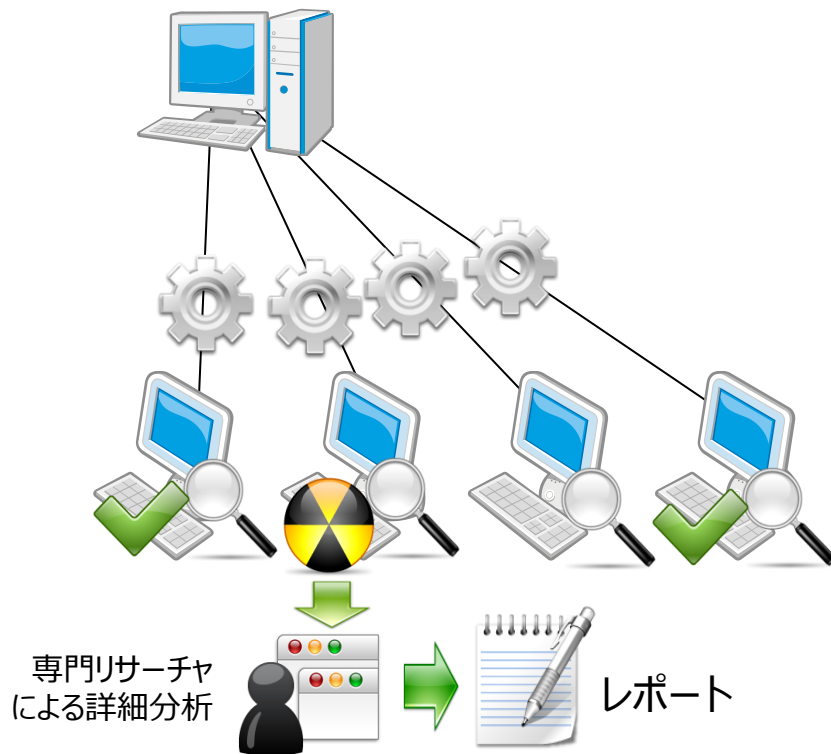
- 標的型攻撃による機密情報漏洩は、時に事業継続上重大なインシデントとなる可能性がある
- しかし既存の技術では発見・防御が困難であり、そのリスクが表面化しにくい状況

このため、標的型攻撃はさまざまなサイバー脅威の中で「最も見えにくい脅威」の一つと言われている

サービス概要

標的型攻撃マルウェアはアンチウイルスでは検出困難

- ・ 標的型攻撃マルウェアが潜んでいる可能性があっても、確認手段がない
- ・ 情報漏洩等が継続的に発生していても、確認手段がない
- ・ 標的型攻撃マルウェアについては各種ログの検査でも発見困難、確認手段がない



標的型攻撃マルウェア検査サービスでスポット検査、確認可能

- ・ 標的型攻撃 マルウェア対策に特化した検出ツール（FFR yarai scanner）を利用
- ・ 各端末をスキャンし情報を収集
- ・ 得られた結果を分析し、確認（誤検知分析、マルウェア分析）

サービス内容

標的型攻撃マルウェアの感染有無を調査

- 標的型攻撃マルウェア検出に特化した高感度の専用検出ツールを使用
 - 標的型攻撃マルウェアが存在するのか否か
 - そのマルウェアが何を行い、どのような被害が発生しているのか
 - 懸念されている被害で発生していないものは何か

被害が発生している場合は対策立案や外部への報告・発表を含めた事後対応を強力にサポート

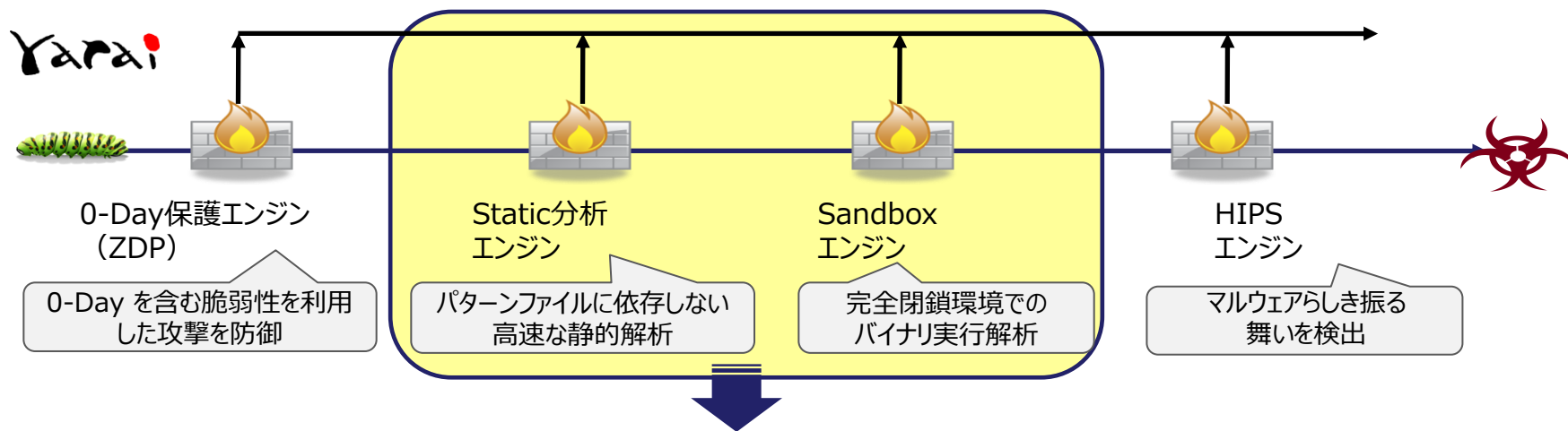
- マルウェアの疑いが強いと判定されたファイルについては、専門アナリストによる詳細解析（リバースエンジニアリング）を実施し、脅威分析を行う
- 標的型攻撃による機密情報漏洩のリスクを可視化対策検討含め、標的型攻撃に対する適切なリスク管理の実現を支援

標的型攻撃マルウェア検出ツール FFR yarai scanner

FFR yarai scannerは、端末にインストールすることなく、クライアントやサーバー内の標的型攻撃マルウェアを検出することができます。

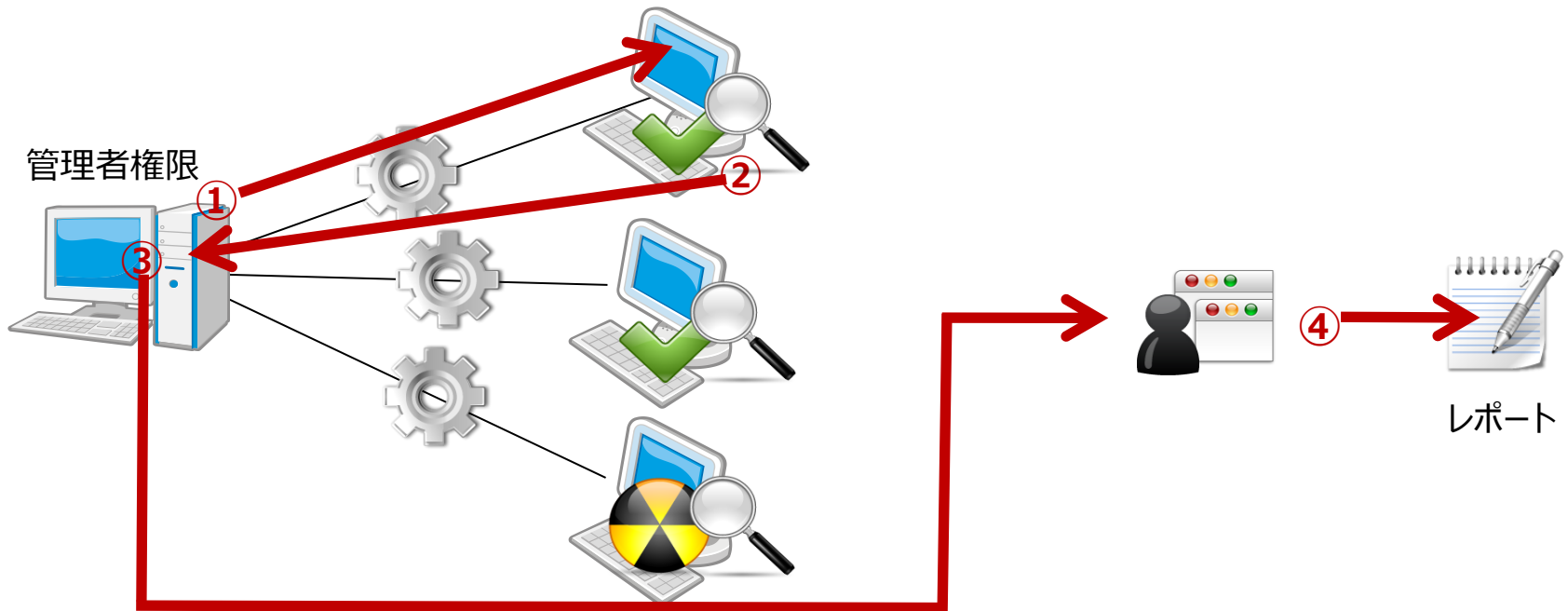
FFR yarai scannerでは、FFR yaraiの以下の4つのエンジンのうち、Static分析エンジンとSandboxエンジンを高感度にチューニングし、使用しています。

※他のZDPIエンジン及びHIPSエンジンはインストールが必要なため検出ツールとしては使用できません。



標的型攻撃マルウェア検出用に
検知精度を上げるチューニングを実施
FFR yarai scanner

検査実施イメージ



- ① FFR yarai scannerを配布し、各端末にて実行します。
- ② FFR yarai scannerは各機器のHDDをスキャンし情報を収集、スキャン結果が管理サーバーに収集されます。
- ③ 管理サーバーに集まったスキャン結果を、専門リサーチャーが分析（誤検知分析・マルウェア分析）します。
（※マルウェアの詳細解析はオプションです。）
- ④ 検査結果をレポートにまとめ、報告会を実施します。

FFR yarai scanner 動作環境

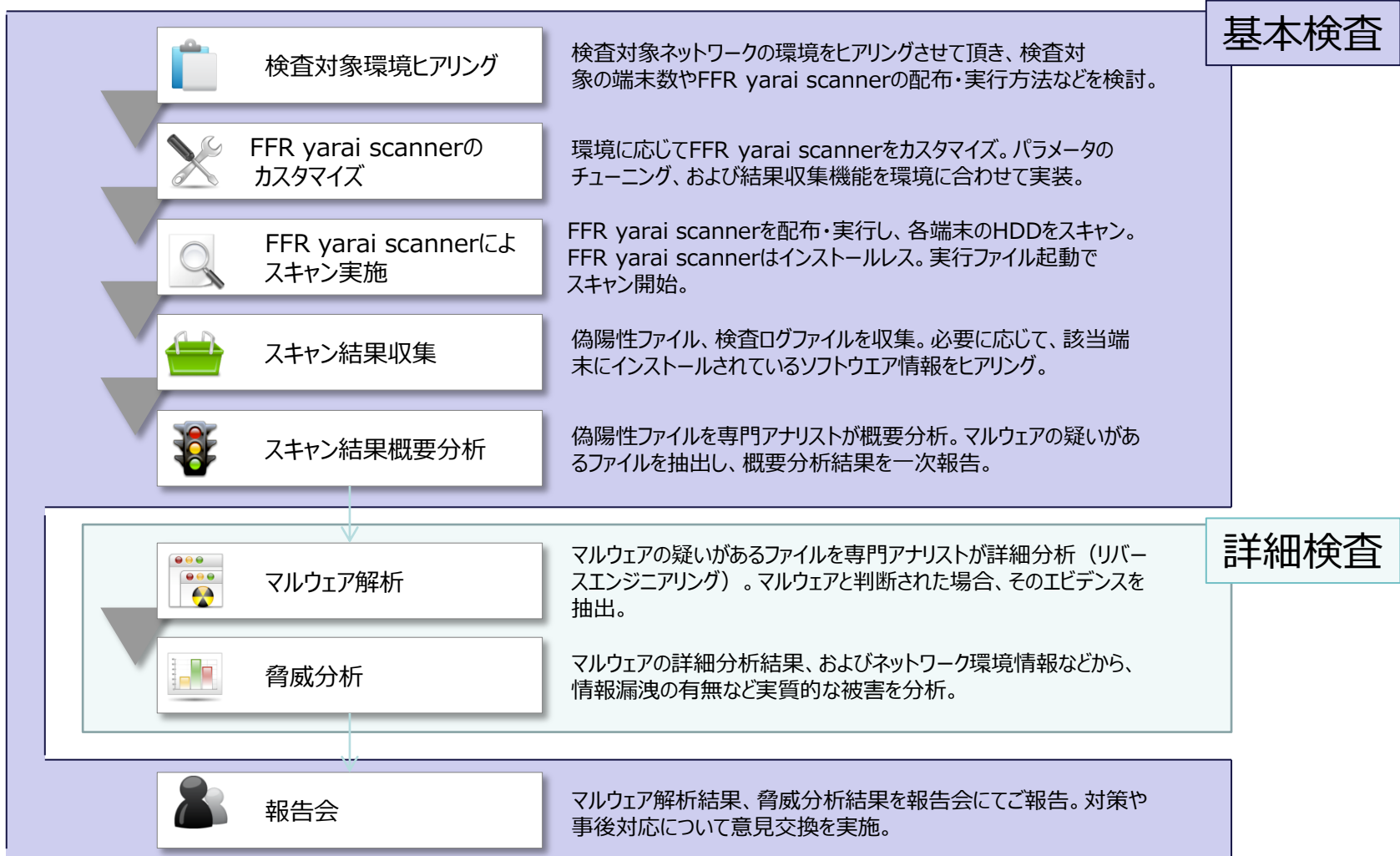
対応OS	
クライアント	Windows 2000 : Professional ※ServicePack3以上 Windows XP : Home, Professional, Media Center, Tablet PC ※ServicePack2以上 Windows Vista : Home Basic, Home Premium, Business, Enterprise, Ultimate Windows 7 : Starter, Home Premium, Professional, Enterprise, Ultimate (32bit/64bit)
サーバー	Windows Server 2000 : Standard, Advanced Server ※ServicePack3以上 Windows Server 2003 : Standard, Enterprise, Datacenter Windows Server 2003 R2 : Standard, Enterprise, Datacenter ※ServicePack2以上 Windows Server 2008 : Standard, Enterprise, Datacenter Windows Server 2008 R2 : Standard, Enterprise, Datacenter

※検査を実施するためには、検査対象端末のHDDの空き容量が200MB以上である必要があります。

※スキャン速度は、500ファイル/分が目安となりますが、環境により実際の速度は前後します。

サービスフローとメニュー構成

標的型攻撃マルウェア検査サービスは、「**基本検査**」と「**詳細検査**」から構成されています。



GSX

GLOBAL
SECURITY
EXPERTS